Google Web Images Groups News Froogle more »
function block security Search Advanced Search Preferences

Web Results **1** - **10** of about **2,340,000** for **function block security**. (**0.54** seconds)

Hash **Functions** and **Block** Ciphers
... Calling the mixing **function** 1 time isn't **secure**. ... Designing **block** ciphers is like that. Sufficient **security** is easy, it's just a question of performance, and of ...
burtleburtle.net/bob/hash/ - 15k - Cached - Similar pages

Bellare - CBC
The **security** of the cipher **block** chaining message authentication code. ... the following general lemma: that cipher **block** chaining a pseudorandom **function** gives a ...
www.cs.ucsd.edu/users/mihir/papers/cbc.html - 3k - Cached - Similar pages

Luby-Rackoff backwards: Increasing **security** by making **block** ...
... invertibility of a **block** cipher can reduce the **security** of schemes ... is the non-invertible analog of a **block** cipher, that is, a pseudorandom **function** (PRF). ...
www.cs.ucsd.edu/users/mihir/papers/p2f.html - 3k - Cached - Similar pages
[More results from www.cs.ucsd.edu]

Administration and Programming Guide
... Calling **Functions**; Calling Net.Data Built-in **Functions**; ... Logic: IF **Blocks**; Looping Constructs: WHILE **Blocks** ... for Handling Error Conditions; **Security**; Direct Call ...
www-306.ibm.com/software/ data/net.data/docs/noframes/400/ - 12k - Cached - Similar pages

Administration and Programming Guide for OS/400

... Calling Net.Data Built-in **Functions**; Generating Web ... Looping Constructs: WHILE **Blocks** ... Handling Error Conditions; **Security**; Direct Call Language Environment; Calling ...
www-306.ibm.com/software/data/ net.data/docs/noframes/400/dtwa2m02.htm - 13k - Cached - Similar pages

RSA **Security** - 2.1.6 What is a hash **function**?
... into **blocks** whose length depends on the compression **function**, and ``padded'' (for **security** reasons) so the size of the message is a multiple of the **block** size. ...
www.rsa**security**.com/rsalabs/faq/2-1-6.html - 15k - Nov 13, 2004 - Cached - Similar pages

C [**Security**]
... cryptography The art and science of information **security**. ... data formats and perform their **function** in the ... algorithm (for example, the RC2 **block** cipher), their ...
msdn.microsoft.com/library/ en-us/secgloss/**security**/c_gly.asp - 31k - Cached - Similar pages

The Hashing **Function** Lounge
... A very nice and deep analysis of the **security** of several hash **function** constructions based on **block** ciphers can be found in BRS02. ...
planeta.terra.com.br/informatica/ paulobarreto/hflounge.html - 23k - Cached - Similar pages

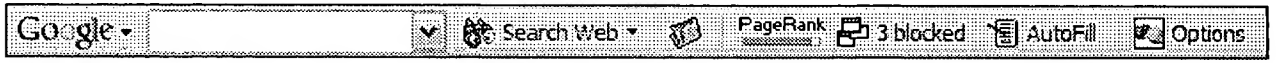
Block Ciphers (part 1)
... with many **block** ciphers there are some keys that should ... Design for an Extended DES", in Computer **Security** in the ... a particular **function** is selected by bits 1,6; ...
williamstallings.com/Extras/ Security-Notes/lectures/**block**A.html - 26k - Cached - Similar pages

Block Ciphers (part 2)
... its overall **security** is currently unknown. ... a one-way hash **function** capable of reducing a message to 64 ... JL Massey, "A Proposal for a New **Block** Encryption Standard ...
williamstallings.com/Extras/ Security-Notes/lectures/**block**B.html - 37k - Cached - Similar pages

Gooooooooooogle ▶

Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

Free! Get the Google Toolbar. Download Now - About Toolbar



function block security Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google

Terms used **function block secure customer** Found **40,988** of **145,831**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown Relevance scale

1 A comment on the confinement problem

Steven B. Lipner

November 1975 **Proceedings of the fifth ACM symposium on Operating systems principles**

Full text available: pdf(435.94 KB) Additional Information: full citation, abstract, references, citings, index terms

The confinement problem, as identified by Lampson, is the problem of assuring that a borrowed program does not steal for its author information that it processes for a borrower. An approach to proving that an operating system enforces confinement, by preventing borrowed programs from writing information in storage in violation of a formally stated security policy, is presented. The confinement problem presented by the possibility that a

borrowed program will modulate its resource usage to t ...

Keywords: Confinement, Leakage of data, Proprietary program, Protection, Security

2 Secure networks: SPV: secure path vector routing for securing BGP

Yih-Chun Hu, Adrian Perrig, Marvin Sirbu

August 2004 **Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications**

Full text available: pdf(236.82 KB) Additional Information: full citation, abstract, references, index terms

As our economy and critical infrastructure increasingly relies on the Internet, the insecurity of the underlying border gateway routing protocol (BGP) stands out as the Achilles heel. Recent misconfigurations and attacks have demonstrated the brittleness of BGP. Securing BGP has become a priority.In this paper, we focus on a viable deployment path to secure BGP. We analyze security requirements, and consider tradeoffs of mechanisms that achieve the requirements. In particular, we study how to se ...

Keywords: BGP, Border Gateway Protocol, interdomain routing, routing, security

3 Advertising and Security for E-Commerence: A lightweight protocol for the generation and distribution of secure e-coupons

Carlo Blundo, Stelvio Cimato, Annalisa De Bonis

May 2002 **Proceedings of the eleventh international conference on World Wide Web**

Full text available: pdf(189.77 KB) Additional Information: full citation, abstract, references, index terms

A form of advertisement which is becoming very popular on the web is based on electronic coupon (e-coupon) distribution. E-coupons are the digital analogue of paper coupons which are used to provide customers with discounts or gift in order to incentive the purchase of

some products. Nowadays, the potential of digital coupons has not been fully exploited on the web. This is mostly due to the lack of "efficient" techniques to handle the generation and distribution of e-coupons. In this paper we d ...

Keywords: accountability, e-commerce, e-coupons, security

4 Secure password-based cipher suite for TLS

May 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 2

Full text available: pdf(507.57 KB) Additional Information: full citation, abstract, references, citings, index terms, review

SSL is the de facto standard today for securing end-to-end transport on the Internet. While the protocol itself seems rather secure, there are a number of risks that lurk in its use, for example, in web banking. However, the adoption of password-based key-exchange protocols can overcome some of these problems. We propose the integration of such a protocol (DH-EKE) in the TLS protocol, the standardization of SSL by IETF. The resulting protocol provides secure mutual authentication and key establi ...

Keywords: Authenticated key exchange, dictionary attack, key agreement, password, perfect forward secrecy, secure channel, transport layer security, weak secret

5 Cellular and Cryptographic Applications: Cryptographic rights management of FPGA intellectual property cores

Tom Kean

February 2002 **Proceedings of the 2002 ACM/SIGDA tenth international symposium on Field-programmable gate arrays**

Full text available: pdf(171.79 KB) Additional Information: full citation, abstract, references, index terms

As the capacity of FPGA's increases to millions of equivalent gates the use of Intellectual Property (IP) cores becomes increasingly important to control design complexity. FPGA's are becoming platforms for integrating a system solution from components supplied by independent vendors in the same way as printed circuit boards provided a platform for earlier generations of designers. However, the current commercial model for IP cores involves large up-front license fees reminiscent of ASIC NRE cha ...

Keywords: FPGA, cryptography, intellectual property, rights management

6 Analysis of packet networks having contention-based reservation with application to GPRS

John N. Daigle, Marcos Nascimento Magalhães

August 2003 **IEEE/ACM Transactions on Networking (TON)**, Volume 11 Issue 4

Full text available: pdf(801.23 KB) Additional Information: full citation, abstract, references, index terms, review

In this paper, we develop a model to quantify the performance of message transmission systems in which users must reserve transmission resources via a contention mechanism prior to transmission. Our work is motivated by a desire to understand the performance characteristics of systems such as the General Packet Radio Service (GPRS), where the single forward link of the wireless access system is organized as a sequence of frames, each of which has first a contention period and then a service peri ...

Keywords: General Packet Radio Service (GPRS), Markov renewal processes, cellular communications, communication networks, contention protocols, performance analysis, queueing systems, wireless communications

7

A nested transaction model for multilevel secure database management systems
Elisa Bertino, Barbara Catania, Elena Ferrari
November 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 4
Full text available: pdf(560.96 KB) Additional Information: full citation, abstract, references, index terms

This article presents an approach to concurrency control for transactions in a Multilevel Secure Database Management System (MLS/DBMS). The major problem is that concurrency control mechanisms used in traditional DBMSs are not adequate in a MLS/DBMS, since they may be exploited to establish covert channels. The approach presented in this article, which uses single-version data items, is based on the use of nested transactions, application-level recovery, and notification-based locking protocols. ...

Keywords: Nested transactions, concurrency control, covert channels, multilevel secure database management systems

8 A decentralized model for information flow control
Andrew C. Myers, Barbara Liskov
October 1997 **ACM SIGOPS Operating Systems Review , Proceedings of the sixteenth ACM symposium on Operating systems principles**, Volume 31 Issue 5
Full text available: pdf(2.24 MB) Additional Information: full citation, references, citings, index terms

9 Securing ATM networks
Shaw-Cheng Chuang
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**
Full text available: pdf(1.53 MB) Additional Information: full citation, references, index terms

10 Key management for encrypted broadcast

Avishai Wool

May 2000 **ACM Transactions on Information and System Security (TISSEC)**, Volume 3 Issue 2

Full text available: pdf(220.36 KB) Additional Information: full citation, abstract, references, index terms

We consider broadcast applications where the transmissions need to be encrypted, such as direct broadcast digital TV networks or Internet multicast. In these applications the number of encrypted TV programs may be very large, but the secure memory capacity at the set-top terminals (STT) is severely limited due to the need to withstand pirate attacks and hardware tampering. Despite this, we would like to allow the service provider to offer different packages of programs to the users. A user ...

Keywords: conditional access, pay-per-view

11 A secure multicast protocol with copyright protection

Hao-hua Chu, Lintian Qiao, Klara Nahrstedt, Hua Wang, Ritesh Jain

April 2002 **ACM SIGCOMM Computer Communication Review**, Volume 32 Issue 2

Full text available: pdf(301.97 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a simple, efficient, and secure multicast protocol with copyright protection in an open and insecure network environment. There is a wide variety of multimedia applications that can benefit from using our secure multicast protocol, e.g., the commercial pay-per-view video multicast, or highly secure military intelligence video conference. Our secure multicast protocol is designed to achieve the following goals. (1) It can run in any open network environment. It does not rely on any sec ...

Keywords: copyright protection, key distribution, multicast security, watermark

12 Data privacy: Private collaborative forecasting and benchmarking

Mikhail Atallah, Marina Bykova, Jiangtao Li, Keith Frikken, Mercan Topkara

October 2004 **Proceedings of the 2004 ACM workshop on Privacy in the electronic society**

Full text available: pdf(217.50 KB) Additional Information: full citation, abstract, references, index terms

Suppose a number of hospitals in a geographic area want to learn how their own heart-surgery unit is doing compared with the others in terms of mortality rates, subsequent complications, or any other quality metric. Similarly, a number of small businesses might want to use their recent point-of-sales data to cooperatively forecast future demand and thus make more informed decisions about inventory, capacity, employment, etc. These are simple examples of cooperative benchmarking and (respectiv ...

Keywords: benchmarking, e-commerce, forecasting, privacy, secure multi-party computation, secure protocol

13 Some cryptographic principles of authentication in electronic funds transfer systems

C. H. Meyer, S. M. Matyas

October 1981 **Proceedings of the seventh symposium on Data communications**

Full text available: pdf(1.22 MB) Additional Information: full citation, abstract, references, index terms

One essential requirement of an Electronic Funds Transfer (EFT) system is that institutions must be able to join together in a common EFT network such that a member of one institution can initiate transactions at entry points in the domain of another institution. The use of such a network is defined as interchange. Cryptographic implementations are

developed for such a network in such a way as to keep personal verification and message authentication processes at diffe ...

14 SOS: secure overlay services

Angelos D. Keromytis, Vishal Misra, Dan Rubenstein

August 2002 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications**, Volume 32 Issue 4

Full text available: pdf(210.90 KB) Additional Information: full citation, abstract, references, citings, index terms

Denial of service (DoS) attacks continue to threaten the reliability of networking systems. Previous approaches for protecting networks from DoS attacks are reactive in that they wait for an attack to be launched before taking appropriate measures to protect the network. This leaves the door open for other attacks that use more sophisticated methods to mask their traffic.We propose an architecture called Secure Overlay Services (SOS) that proactively prevents DoS attacks, geared toward supportin ...

Keywords: denial of service attacks, network security, overlay networks

15 Digital signets: self-enforcing protection of digital information (preliminary version)

Cynthia Dwork, Jeffrey Lotspiech, Moni Naor

July 1996 **Proceedings of the twenty-eighth annual ACM symposium on Theory of computing**

Full text available: pdf(1.24 MB) Additional Information: full citation, references, citings, index terms

16 Software engineering for security: a roadmap

Premkumar T. Devanbu, Stuart Stubblebine
May 2000 **Proceedings of the Conference on The Future of Software Engineering**
Full text available: pdf(1.71 MB) Additional Information: full citation, references, citings, index terms

Keywords: copy protection, security, software engineering, water-marking

17 Cryptographic verification of test coverage claims
Prem Devanbu, Stuart G. Stubblebine
November 1997 **ACM SIGSOFT Software Engineering Notes , Proceedings of the 6th European conference held jointly with the 5th ACM SIGSOFT international symposium on Foundations of software engineering**, Volume 22 Issue 6
Full text available: pdf(1.67 MB) Additional Information: full citation, references, citings, index terms

18 Electronic commerce: a half-empty glass?
Sasa Dekleva
June 2000 **Communications of the AIS**
Full text available: pdf(343.49 KB) Additional Information: full citation, references

19 Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world
Marjory S. Blumenthal, David D. Clark
August 2001

ACM Transactions on Internet Technology (TOIT), Volume 1 Issue 1

Full text available: pdf(176.33 KB) Additional Information: full citation, abstract, references, citings, index terms

This article looks at the Internet and the changing set of requirements for the Internet as it becomes more commercial, more oriented toward the consumer, and used for a wider set of purposes. We discuss a set of principles that have guided the design of the Internet, called the end-to-end arguments, and we conclude that there is a risk that the range of new requirements now emerging could have the consequence of compromising the Internet's original design principles. Were ...

Keywords: ISP, Internet, end-to-end argument

20 A secure and private system for subscription-based remote services

Pino Persiano, Ivan Visconti

November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4

Full text available: pdf(241.65 KB) Additional Information: full citation, abstract, references, index terms

In this paper we study privacy issues regarding the use of the SSL/TLS protocol and X.509 certificates. Our main attention is placed on subscription-based remote services (e.g., subscription to newspapers and databases) where the service manager charges a flat fee for a period of time independent of the actual number of times the service is requested.We start by pointing out that restricting the access to such services by using X.509 certificates and the SSL/TLS protocol, while preserving the in ...

Keywords: Access control, anonymity, cryptographic algorithms and protocols, privacy, world-wide web

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next